DEVELOPING AN ARCHIVE FOR NETWORK ANALYSIS, R. Phelps, L. Hopper, R. Hopper, P.C. Womble*, Cyber Defense Laboratory, Western Kentucky University, Bowling Green, Ky 42261, womble@wku.edu

The Cyber Defense Laboratory at Western Kentucky University is developing a repository of network traffic patterns to aid in the efforts of the network analysis community. The archive will consist of packet capture files, along with detailed event logs, timelines, and descriptions. Individual packets within captured traffic data may also be marked via changes to protocol numbers within the unassigned range (140-252) to highlight the significance of certain packets within the capture. Each will be searchable and in a standardized format that is currently in development. All data sets and submissions to the archive will be prepared by an editor and archivist; experts in the field will be able to submit their own data to the archive after a process of peer review. The high quality standards of the archive and frequent submission of additional data will help make it a valuable tool for research in the network analysis community.